JP Journal of Algebra, Number Theory and Applications
Volume 15, Number 1, 2009, Pages 19-28
This paper is available online at http://www.pphmj.com

DECOMPOSITION OF MODULES

HIROYUKI ISHIBASHI

Department of Mathematics
Josai University
Sakado, Saitama 350-02, Japan
e-mail: hishi@math.josai.ac.jp

Abstract

Our first purpose is to give a sufficient condition for modules over rings to be expressed as a sum or a direct sum of submodules of the modules without any special restriction for modules and rings. Then we will apply the result to various cases of modules and rings.

For example, we will realize a generalization of the fact that an involutary endomorphism of a module gives rise to a splitting of the module into a direct sum of two submodules.

Also, we shall show that the existence of an idempotent linear endomorphism in a wide meaning allows us to split the underlying module.

1. Introduction

Let E be a module over a ring R. We wish to start our investigation of splitting modules over rings under as weak condition as possible.

So, in our proposition which is the first result of our study, we will set no assumption for the underlying ring R other than it is associative and unitary. Also, a module E will be assumed to be neither free nor finitely generated.

2000 Mathematics Subject Classification: 13C05, 13C10, 13C12, 15A04, 15A23, 15A33.

Keywords and phrases: decomposition of modules, direct sum of modules, annihilator ideal, involution, idempotent, structure theorem of finitely generated modules over PID, endomorphisms ring of modules, classical groups.

Received September 12, 2009

In this situation, in our proposition we shall show that the existence of two distinguished elements a, b in R possessing a nice property gives us a splitting of E as a sum or a direct sum of two submodules of E.

Then we will use the proposition to perform splittings of modules under various conditions for modules and rings. Since the results will be stated and proved as Theorems A to E in the next section, we will here just try to do a brief description of the theorems.

In Theorem A, we shall show that if two endomorphisms f, g of a module M satisfy some conditions, then we will have a splitting

$$M = \ker f \oplus \ker g.$$

Theorem B is a special case of Theorem A, where we will restrict ourselves to the case $R = S[\sigma]$, a ring extension of a commutative ring S by an endomorphism σ of a module M over S, and show that the same result as Theorem A under weaker conditions.

Theorem C is an application of the proposition to a vector space and have an well-known result that a factorization of the minimal polynomial of an endomorphism gives a splitting of the underlying module. However, in our proof, we will not use the structure theorem of finitely generated module over PID.

A linear endomorphism f of a vector space V over a field k is called an *involution* on V if $f^2 = 1$, the identity map on V. We know that if $\operatorname{char} k \neq 2$ and f is an involution on V, V is split into a direct sum of two subspaces $V_f = \{x \in V \mid f(x) = x\}$ and $V_{-f} = \{x \in V \mid f(x) = -x\}$ of V. Theorem D is a generalization of this fact.

Our main result is Theorem E, in which we choose a linear endomorphism f of a module M and show that if f is an idempotent element in a wide meaning, that is, if f satisfies $f^2 = \varepsilon f$ for a central unit ε in the coefficient ring R of M, then M can be expressed as a direct sum of two submodules.

Hahn and O'Meara [1] is an outstanding book on the theory of classical groups and K-theory. Also, in Knus [5], we can see a modern conceptual approach to classical groups. In McDonald [7], he established the theory of classical groups over local rings. Ishibashi [3] is a graph theoretical treatment for generation of the

symplectic groups and give a necessary and sufficient condition for a certain class of subsets to generate the whole group. In Ishibashi [2, 3], we factorize linear endomorphisms into a product of involutions or semiinvolutions and estimate the small number of factors. Lang [6] is a standard text book in algebra and the reader can consult it for concepts or materials seen in this paper.

2. Statements and Proofs of Proposition and Theorems

Now, in the present section, we will state our proposition and Theorems A, B, C and D in the explicit form and prove them.

Proposition. *Let R be a ring and E be a left module over R. Then the following* (a) *and* (b) *hold*:

(a) *If two elements a, b in R satisfy*

(i) $abE = baE = 0$ *and* (ii) $aR + bR = R$,

then we have

(1) $E = E_a + E_b$

for $E_a = \{x \in E \mid ax = 0\}$ *and* $E_b = \{y \in E \mid by = 0\}$.

(b) *Further, if an additional condition*

(iii) *a, b are central elements of R*

is satisfied, then we have

(2) $E = E_a \oplus E_b$.

Proof. First, we prove (a). By (ii), we have $aR + bR = R$. Hence, for some c, d in R,

$$ac + bd = 1$$

holds.

This implies that for any x in E,

$$acx + bdx = x.$$

Further, if we use (i), then we understand that

$$acx \in E_b \quad \text{and} \quad bdx \in E_a,$$

which gives us

(1) $E = E_a + E_b$.

Next, we show (b). If not only (i) and (ii) but (iii) is also satisfied, for any x in $E_a \cap E_b$, we get

$$x = acx + bdx = cax + dbx = 0 + 0 = 0.$$

Hence

(2) $E = E_a \oplus E_b$,

which was to be shown. □

Theorem A. *Let S be a ring, M be a left module over S, $End_S M$ be the endomorphism ring of M, and f, g be elements in a subring R of $End_S M$. Then we have the following* (a) *and* (b):

(a) *If*

(i) $fgM = gfM = 0$ *and* (ii) $fR + gR = R$,

are satisfied, then we have

(1) $M = \ker f + \ker g$.

(b) *If additionally*

(iii) *f, g are in the center of R*

is satisfied, then we have

(2) $M = \ker f \oplus \ker g$.

Proof. Define an action $\cdot$ of R on M by

$$f \cdot x = f(x) \quad \text{for} \quad f \in R \quad \text{and} \quad x \in M.$$

Then M is endowed a left R-module structure. Therefore, applying (a) of the proposition, we have

$$M = M_f + M_g.$$

However, since $M_f = \ker f$ and $M_g = \ker g$, this shows that

$$M = \ker f + \ker g.$$

Further, if (iii) of the theorem is satisfied, then by (b) of the proposition, we have

$$M = \ker f \oplus \ker g. \qquad \square$$

Theorem B. *In Theorem* A, *let S be a commutative ring acting faithfully on M, and R be an extension of S by an element* σ *in* $End_S M$, *that is,* $R = S[\sigma]$. *Then if f, g in R satisfy*

$$fg = 0 \quad and \quad fR + gR = R,$$

we have

$$M = \ker f \oplus \ker g.$$

Proof. In our situation *R* is commutative, so the theorem is straightforward by Theorem A. $\square$

For a ring *S* and an indeterminate *t* a formal power series

$$\sum_i a_i t^i = a_0 + a_1 t + a_2 t^2 + \cdots, \quad a_i \in S$$

is called a *polynomial* in *t* with coefficients in *S* if $a_N = a_{N+1} = \cdots = \cdots = 0$ for some *N* in $\{0, 1, 2, ...\}$. For two polynomials $f(t) = \sum_i a_i t^i$ and $g(t) = \sum_i b_i t^i$, we define

(i) equality: $f(t) = g(t)$ if and only if $a_i = b_i$, for all *i*,

(ii) addition: $f(t) + g(t) = \sum_i (a_i + b_i) t^i$,

and

(iii) multiplication: $f(t)g(t) = \sum_i \left(\sum_{i=p+q} a_p b_q \right) t^i$.

Then the set of polynomials form a ring, which we call a *polynomial ring* in *t* with coefficients in *S*, and denote it by $S[t]$. Since $0t^i = 0$ for $i = 0, 1, 2, ...,$ any polynomial is expressed as a finite sum of terms.

Also, since *S* is embedded in $S[t]$, we may assume that *S* is a subring of $S[t]$, and $S[t]$ is generated by *t* over *S*. Clearly, if *S* is commutative, so is $S[t]$.

Theorem C. *Let k be a field and $k[t]$ be the polynomial ring in t over k. Let V be finite dimensional vector space over k, and $End_k V$ be the endomorphism ring of V over k. Further, for $\sigma \in End_k V$ let $g(t)$ in $k[t]$ be the monic minimal polynomial of σ with $\deg g(t) \geq 1$. Then for a factorization*

$$g(t) = p_1(t)^{e_1} p_2(t)^{e_2} \cdots p_r(t)^{e_r}$$

with $p_1, p_2, ..., p_r$ irreducible in $k[t]$ and $e_1, e_2, ..., e_r$ natural numbers, we have a splitting

$$V = \ker p_1^{e_1}(\sigma) \oplus \ker p_2^{e_2}(\sigma) \oplus \cdots \oplus \ker p_r^{e_r}(\sigma).$$

Proof. If we define an action of $k[t]$ on V by

$$f(t)x = f(\sigma)x \quad \text{for} \quad f(t) \in k[t] \quad \text{and} \quad x \in V,$$

V is regarded as a $k[t]$-module. Further, since k is a field, if we set in the proposition

$$R = k[t], \quad E = V, \quad a = p_1(t)^{e_1} \quad \text{and} \quad b = p_2(t)^{e_2} \ldots p_r(t)^{e_r},$$

then conditions (i), (ii) and (iii) in the proposition are all satisfied. Consequently, we have

$$V = V_{p_1(t)^{e_1}} \oplus V_{p_2(t)^{e_2} \ldots p_r(t)^{e_r}}.$$

Now, by induction in r, we obtain

$$\begin{aligned} V &= V_{p_1(t)^{e_1}} \oplus V_{p_2(t)^{e_2}} \oplus \cdots \oplus V_{p_r(t)^{e_r}} \\ &= \ker p_1(t)^{e_1} \oplus \ker p_2(t)^{e_2} \oplus \cdots \oplus \ker p_r(t)^{e_r}. \end{aligned}$$ □

Lemma 2.1. *A polynomial $f(t) = \sum a_i t^i$ in $S[t]$ is central in $S[t]$ if and only if so is each a_i in S.*

Proof. Suppose that a coefficient a_k of $f(t)$ is not central. Then there is b in S such that $a_k b \neq b a_k$. Therefore, for $g(t) = b$, we have

$$fg = \left(\sum a_i t_i\right) b = \sum a_i b t^i \neq \sum b a_i t^i = b\left(\sum a_i t^i\right) = gf,$$

which shows that f is not central in $S[t]$. Thus, if f is central, so are all a_is. The converse is clear. □

Theorem D. *Let S be a ring with* 2 *a unit, M be a module over S, and* $End_S M$ *be the endomorphism ring of M over S. Then for* σ *in* $End_S M$ *if* $\sigma^{2^n} = 1$, *we have a splitting*

$$M = M_\sigma \oplus M_{-\sigma} \oplus M_{-\sigma^2} \oplus \cdots \oplus M_{-\sigma^{2^{n-1}}},$$

where $M_\tau = \{x \in M \mid \tau x = \tau\}$ *for any* τ *in* $End_S M$, *i.e., the fixed module of* τ *in M.*

Proof. If $n = 0$, then we have $\sigma = 1$ and $M = M_\sigma$, hence the theorem holds. So, we prove it by induction on *n*. Let $R = S[t]$ be the polynomial ring in *t* over *S*. Then as in the proof for Theorem C, *M* is a module over *R* by defining $f(t)x = f(\sigma)x$ for *x* in *M* and $f(t)$ in *R*. Since $\sigma^{2^n} = 1$, we have $(\sigma^{2^{n-1}} + 1)(\sigma^{2^{n-1}} - 1) = 0$.

Therefore, if we write

$$f = t^{2^{n-1}} + 1 \quad \text{and} \quad g = t^{2^{n-1}} - 1,$$

then we have

(i) $fgM = gfM = 0$.

Since 2 is a unit in *S*, we have $2^{-1}f - 2^{-1}g = 1$, hence

(ii) $Rf + Rg = R$.

Further, since the coefficients ± 1 of *f* and *g* are in the center of *S*, by the lemma, we have

(iii) $f(t)$ and $g(t)$ in the center of $S[t]$.

So, applying the proposition, we obtain

$$M = M_{\sigma^{2^{n-1}}} \oplus M_{-\sigma^{2^{n-1}}}.$$

Now, the inductive hypothesis gives us the expression of *M* as in the theorem. □

Theorem E. *Let S be a ring, M be a left module over S, and* $End_S M$ *be the endomorphism ring of M. Further, for* σ *in* $End_S M$ *assume that*

$$\sigma^2 = \varepsilon\sigma \quad \textit{for } \varepsilon \textit{ a central unit in } S.$$

Then we have

(a) $\ker \sigma = \mathrm{Im}(\sigma - \varepsilon 1_M)$, $\mathrm{Im}\,\sigma = \ker(\sigma - \varepsilon 1_M)$,

and

(b) $M = \ker \sigma \oplus \mathrm{Im}\,\sigma$,

where 1_M *is the identity transformation on M.*

Proof. Let R be the polynomial ring in t over S, i.e., $R = S[t]$. In the same way, as the proof for Theorem C, if we define an action of R on M by

$$f(t)x = f(\sigma)x \quad \text{for} \quad f(t) \in R \quad \text{and} \quad x \in M,$$

then M becomes a left module over R.

Further, if we set two elements f, g in R as

$$f = t \quad \text{and} \quad g = t - \varepsilon,$$

then we have

(i) $fgM = gfM = 0$.

Since $f - g = \varepsilon$ is a unit in S, we also have

(ii) $fR + gR = R$.

To show that f and g are central elements in R choose any h in R and write

$$h = \sum a_i t^i, \quad a_i \in S.$$

Then it is easy to see that

(1) $$fh = t\left(\sum a_i t^i\right) = \sum a_i t^{i+1} = \left(\sum a_i t^i\right) t = hf,$$

hence f is central. Next, since ε is a central element in S, we have

$$\varepsilon h = \varepsilon\left(\sum a_i t^i\right) = \sum \varepsilon a_i t^i = \sum a_i \varepsilon t^i = \left(\sum a_i t^i\right)\varepsilon = h\varepsilon.$$

Therefore,

(2) $gh = (t - \varepsilon)h = h(t - \varepsilon) = hg$.

So, we conclude that

(iii) f, g are central elements in R.

Then our proposition yields that

(3) $M = M_f \oplus M_g = \ker\sigma \oplus \ker(\sigma - \varepsilon \cdot 1_M)$.

Therefore, if we have verified (a) of the theorem, then we will obtain (b).

Thus, the rest to be shown is (a) of the theorem. Since $\sigma^2 = \varepsilon\sigma$, we have $(\sigma - \varepsilon 1_M)\sigma = 0$, which gives us

(4) $\operatorname{Im}\sigma \subseteq \ker(\sigma - \varepsilon 1_M)$.

To show the converse, since $\ker(\sigma - \varepsilon 1_M) \subseteq M$, we have

$$\sigma \ker(\sigma - \varepsilon 1_M) \subseteq \sigma M = \operatorname{Im}\sigma.$$

Here, rearranging the left hand side of the inclusion, we have

$$\sigma \ker(\sigma - \varepsilon 1_M) = (\varepsilon 1_M + (\sigma - \varepsilon 1_M)) \ker(\sigma - \varepsilon 1_M)$$

$$= \varepsilon \ker(\sigma - \varepsilon 1_M).$$

Further, since ε is a unit in S, we obtain

$$\varepsilon \ker(\sigma - \varepsilon 1_M) = \ker(\sigma - \varepsilon 1_M).$$

So, we get the converse

(5) $\ker(\sigma - \varepsilon 1_M) \subseteq \operatorname{Im}\sigma$,

and by (4), (5), we have the equality

(6) $\operatorname{Im}\sigma = \ker(\sigma - \varepsilon 1_M)$.

In the same way

(7) $\ker\sigma = \operatorname{Im}(\sigma - \varepsilon 1_M)$

is verified.

Thus, we have proved (a) of the theorem, which completes our proof for the theorem. □

References

[1] A. J. Hahn and O. T. O'Meara, The Classical Groups and *K*-theory, Grund. Math. Wissenschaften, 291, Springer-Verlag, Berlin, New York, Tokyo, 1989.

[2] H. Ishibashi, Involutary expressions for elements in $GL_n(\mathbb{Z})$ and $SL_n(\mathbb{Z})$, Linear Algebra Appl. 219 (1995), 165-177.

[3] H. Ishibashi, Groups generated by symplectic transvections over local rings, J. Algebra 218(1) (1999), 26-80.

[4] H. Ishibashi, Involutions and semiinvolutions, Czechoslovak Math. J. 56(131) (2006), 533-541.

[5] M.-A. Knus, Quadratic and Hermitian Forms over Rings, Grund. Math. Wissenschaften, 294, Springer-Verlag, Berlin, New York, Tokyo, 1991.

[6] S. Lang, Algebra, 3rd ed., Addison-Wesley, Tokyo, 1993.

[7] B. R. McDonald, Geometric algebra over local rings, Pure and Applied Mathematics, 36, Marcel Dekker, Inc., New York-Basel, 1976.